Coronavirus (COVID-19) communications
Cyber threat – increased or just different?

HISCOX
CYBERCLEAR®

There have been huge volumes of press recently about the increased threat of cyber-attacks since the outbreak of the COVID-19 pandemic. We think it's important to keep the threat in context.

Some cyber incidents are less likely…

A very common cyber loss scenario is a lost laptop that's unencrypted. It's unlikely in the current environment, however, that anyone is convening in city centre bars and subsequently losing their bag containing a laptop. Also, many companies (Google, Microsoft etc.) have said that due to staffing shortages they will slow down releases or reduce the amount of IT change happening, which would potentially reduce system outage occurrences.

But there are new threats…

1. **Remote working increases attack surface –** as companies roll-out work from home (WFH) solutions, not only are potentially less secure devices being connected to corporate networks, but rapidly rolled out remote access solutions may lack the thorough security testing that would have taken place in more stable times.
2. **Lack of co-worker conversations –** typically when we receive suspicious emails, we might turn to a colleague and ask 'I just got this email, did you get it? Do you think it's suspicious?' This isn't an option currently, so there's a chance that more phishing emails will succeed.
3. **We are all looking for information –** in these uncertain times, we are all looking for answers, there's an increased thirst for information, and therefore are more likely to click on links or articles that we find online or are shared through our social networks.

Are there really more phishing attacks?

There have been number of press releases in the last week, that bring some interesting statistics to the debate:

- Google says it blocked 18 million COVID-19-themed phishing emails targeting Gmail users last week. This would represent about 2.5% of the 100 million phishing emails Google said it blocked daily in 2019.
- Microsoft tracks thousands of email phishing campaigns that cover millions of malicious messages every week. They said recently *"of the millions of targeted messages we see each day, roughly 60,000 include COVID-19-related malicious attachments or malicious URLs"*. While that number sounds very large, it's important to note that it's less than 2% of the total volume of threats we actively track and protect against daily, which reinforces that the overall volume of threats is not increasing. Attackers are, however, shifting their techniques to capitalise on fear.
- Barracuda – recently reported that *"between March 1st and March 23rd, Barracuda Sentinel detected 467,825 spear-phishing email attacks, and 9,116 of those detections were related to COVID-19, which represents about 2% of attacks"*.

It's interesting that all three reports converge on around 2% of all phishing emails being COVID-19-related. This aligns with our belief that existing phishing campaigns have pivoted to using COVID-19 lures rather than the traditional tax rebate, Netflix or Apple lures that we're used to.

COVID-19-related claims

At this stage we've not seen a material number of cyber-related COVID-19 claims, however two interesting and slightly lateral claims are described below.

Example one: in March, a UK based SME had data stolen from a database – estimated to contain approximately 2,000 personal records. The data belongs to a third party who the insured was developing a website for. The attackers requested a ransom in Bitcoin in return for the data. The attack appears to have made use of an open database connection on a desktop machine that was taken home by an employee to work remotely during the COVID-19 lockdown.

Ordinarily the corporate on-premise network firewall would have prevented this connection from being made, but once the machine was physically moved to the home of an employee this firewall protection was no longer applicable. Instead, network security become dependent on the security features of the employee's home router.

The 'so what': this case highlights the need to consider the security impact of moving devices which under normal conditions would not leave a corporate office, and to give consideration for the use of host and network-based firewalls at all times.

Example two: in March, a US company experienced a ransomware attack where all of the servers on its network were encrypted. Although this was discovered in mid-March, investigations show that the attack may have spread from a single infected PC that had been dormant since January 2020. The infected PC was given to an employee (so they could work at home in response to the COVID-19 lockdown) who connected it to the network, which unknowingly caused the ransomware to spread.

The 'so what': this is a good example of why it is important to inspect decommissioned or dormant devices before re-commissioning them for use, even if they've been previously wiped clean by internal IT teams or a third party. It's especially important during this time when many additional and potentially less secure devices are being issued to employees for remote working.

Hiscox
1 Great St Helen's
London EC3A 6HX
United Kingdom

T +44 (0)20 7448 6000
E enquiry@hiscox.com
www.hiscoxgroup.com

20672 04/20